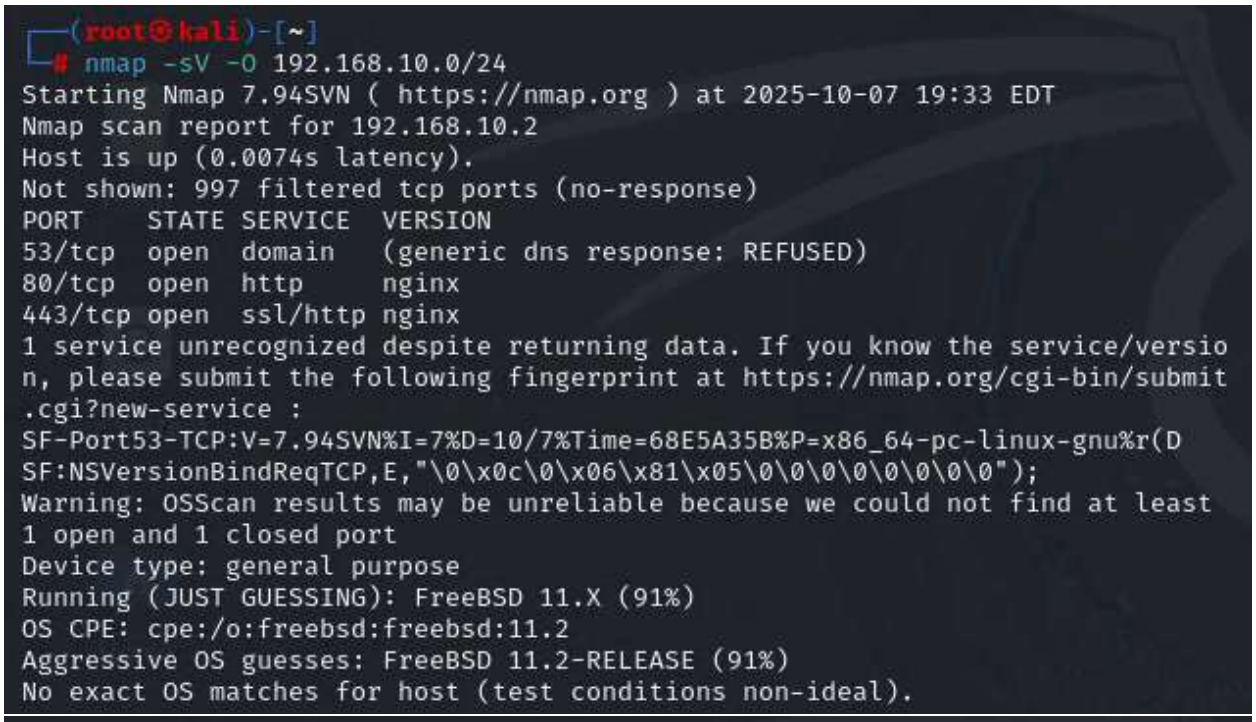
CYSE 301: Cybersecurity Technique and Operations

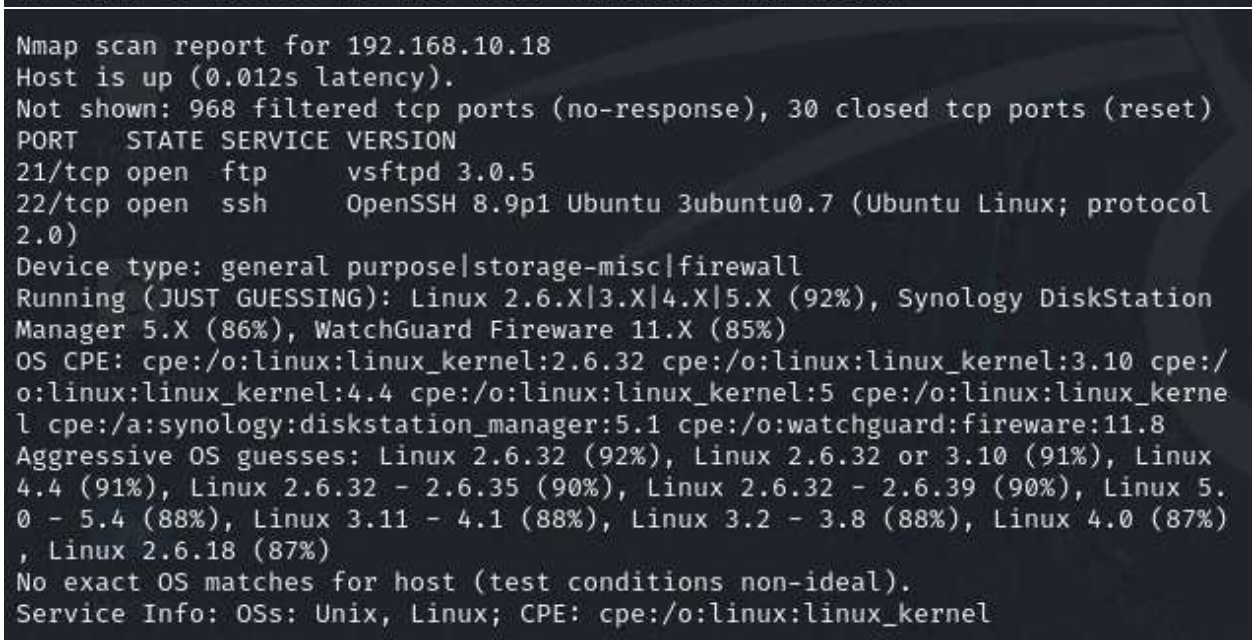
Assignment 3: Sword vs. Shield

Task A: Sword - Network Scanning (20+ 20 = 40 points)

1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.



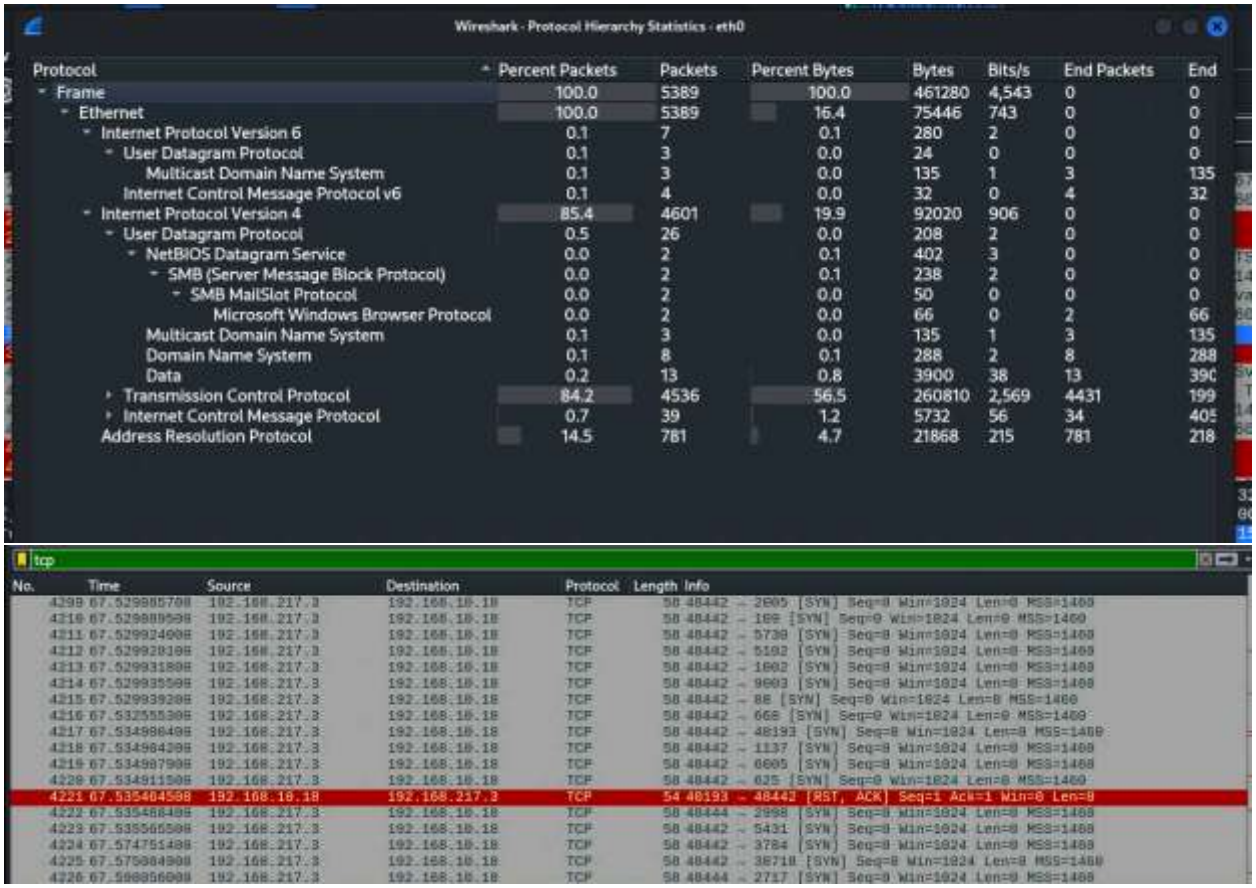
```
┌──(root㉿kali)-[~]
└─# nmap -sV -O 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-07 19:33 EDT
Nmap scan report for 192.168.10.2
Host is up (0.0074s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: REFUSED)
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=10/7%Time=68E5A35B%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
```

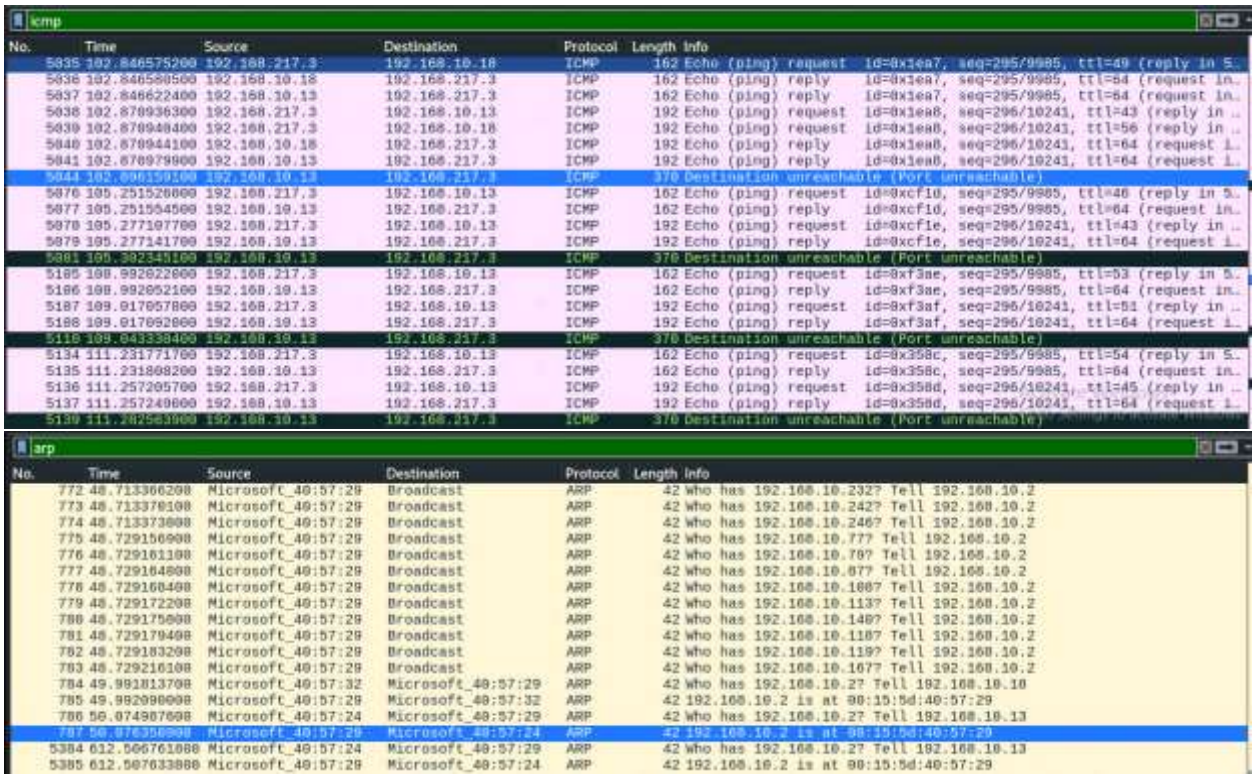


```
Nmap scan report for 192.168.10.18
Host is up (0.012s latency).
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol
2.0)
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X|5.X (92%), Synology DiskStation
Manager 5.X (86%), WatchGuard Fireware 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/
o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kerne
l cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (91%), Linux
4.4 (91%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 5.
0 - 5.4 (88%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 4.0 (87%)
, Linux 2.6.18 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.10.19
Host is up (0.011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows
 11 21H2 (91%), Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 45.53 seconds
```

2. Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**



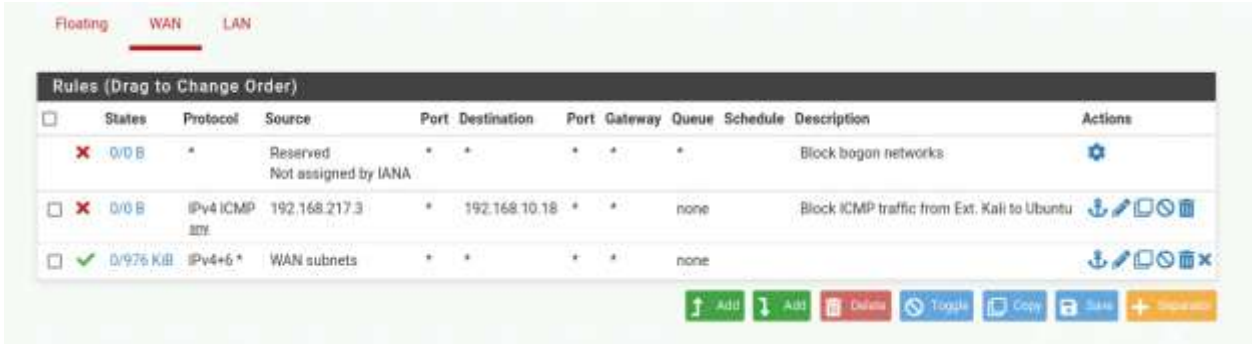


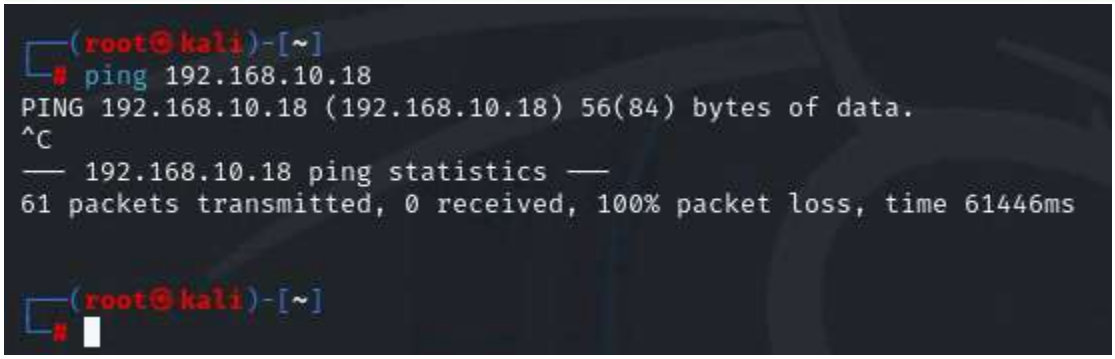
- After scanning the network using nmap on External Kali, the returned traffic pattern was quite vast. As you can see in the above image, 5,389 packets were captured during the nmap scan. Over ¾ of the captured packets were TCP packets with the external kali machine attempting to create a connection with SYN packets. Most of the SYN packets were sent to the internal kali machine, and a small number were sent to the Ubuntu VM. No SYN packets were sent to the Windows Server machine. Most of the SYN packets sent by the external Kali VM were met with RST/ACK packets instead of normal SYN/ACK packets. The RST/ACK packets were sent to indicate an incomplete TCP connection. There was also a small number of ICMP packets (0.7%) sent from the external Kali VM to the internal Kali and Ubuntu VMs. Out of the 39 ICMP packets sent between the VMs, there were 5 packets that were sent from the internal Kali VM to the external Kali VM which stated that the destination and port were unreachable. Additionally, there was a larger number of ARP packets (14.5%) that were sent from the pfsense firewall VM requesting the information associated with certain IP and MAC addresses. (See the above photos for screenshots of TCP, ICMP, and ARP packets).

Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

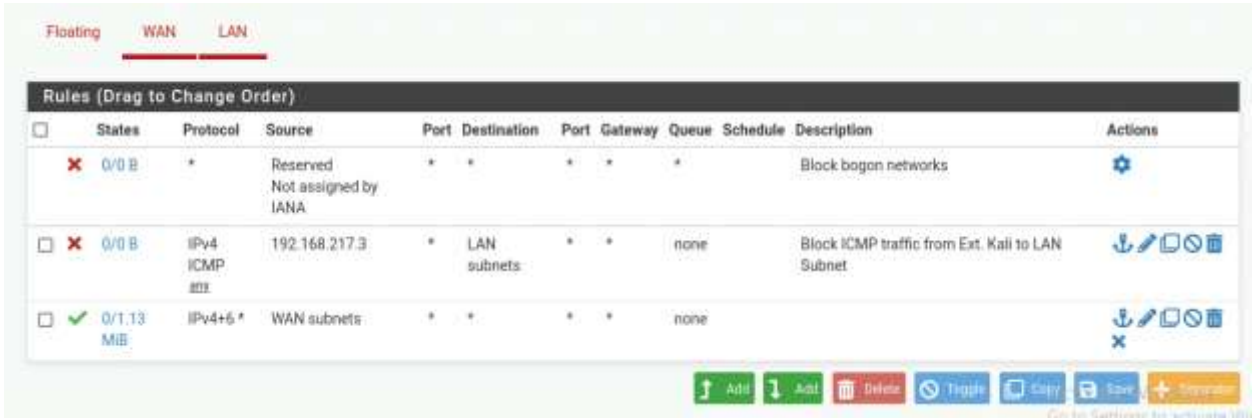
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	block	192.168.217.3	192.168.10.18	ICMP





2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

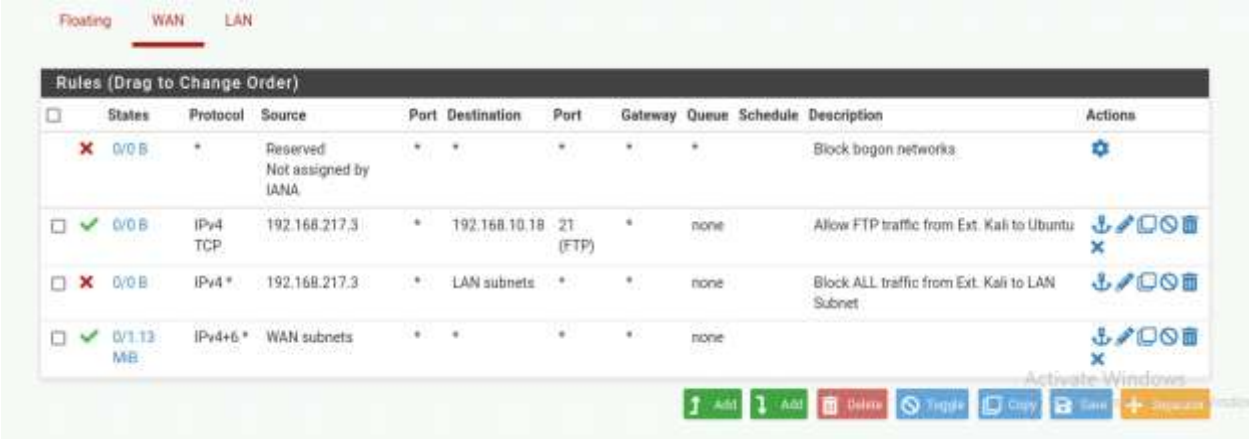
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	192.168.10.0/24 (Subnet IP)	ICMP



```
┌──(root㉿kali)-[~]
└─# ping 192.168.10.13
PING 192.168.10.13 (192.168.10.13) 56(84) bytes of data.
^C
── 192.168.10.13 ping statistics ──
25 packets transmitted, 0 received, 100% packet loss, time 24552ms

┌──(root㉿kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
── 192.168.10.18 ping statistics ──
15 packets transmitted, 0 received, 100% packet loss, time 14319ms

┌──(root㉿kali)-[~]
└─# ping 192.168.10.19
PING 192.168.10.19 (192.168.10.19) 56(84) bytes of data.
^C
── 192.168.10.19 ping statistics ──
17 packets transmitted, 0 received, 100% packet loss, time 16388ms

┌──(root㉿kali)-[~]
└─#
```

3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
3	WAN	Block	192.168.217.3	192.168.10.0/24 (Subnet IP)	Any
4	WAN	Pass	192.168.217.3	192.168.10.18	FTP / Port 21



```
┌──(root㉿kali)-[~]
└─# ping 192.168.10.19
PING 192.168.10.19 (192.168.10.19) 56(84) bytes of data.
^C
── 192.168.10.19 ping statistics ──
13 packets transmitted, 0 received, 100% packet loss, time 12269ms

┌──(root㉿kali)-[~]
└─# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data.
^C
── 192.168.10.18 ping statistics ──
11 packets transmitted, 0 received, 100% packet loss, time 10218ms

┌──(root㉿kali)-[~]
└─# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.

┌──(root㉿kali)-[~]
└─# ftp 192.168.10.19
^C
```

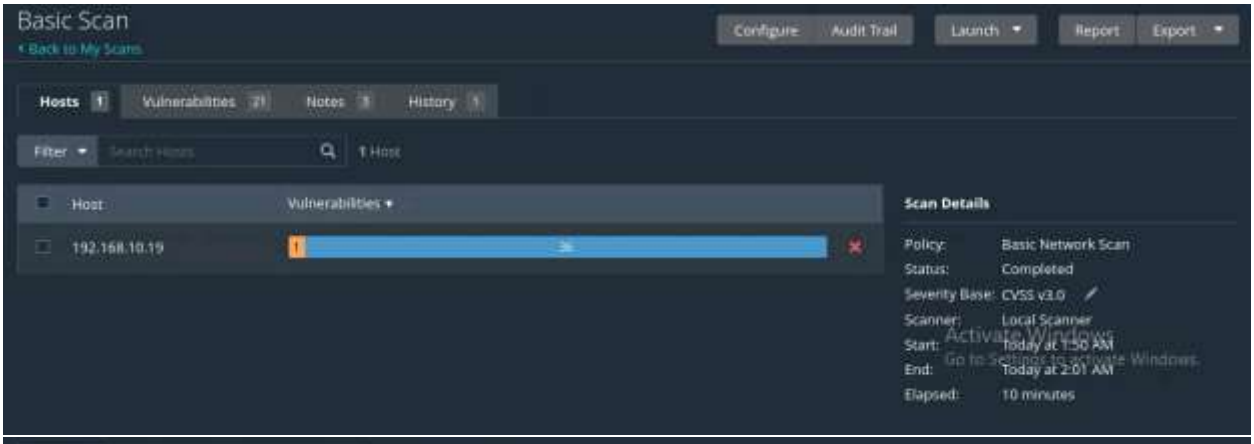
4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

```
┌──(root㉿kali)-[~]
└─# nmap -sV -O 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-08 01:26 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.85 seconds

┌──(root㉿kali)-[~]
└─#
```

- **After attempting to scan the subnet using nmap, the newly added firewall rules were able to block any information from being gathered by the external Kali VM. The scan provided the message that 0 hosts were up despite the internal Kali, Ubuntu, Windows 2022 Server, and pfsense firewall all running during the time of the scan.**

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.

- **I performed a basic scan of the Microsoft Windows Server 2022, and 21 vulnerabilities appeared when the scan finished; 20 of them were basic information and one of them was a medium level vulnerability.**



INFO	Ethernet Card ...	Misc.	1		
INFO	Ethernet MAC A...	General	1		
INFO	Hyper-V Virtual ...	General	1		
INFO	Link-Local Multi...	Service detection	1		
INFO	Nessus Scan Inf...	Settings	1		
INFO	NetBIOS Multip...	Windows	1		
INFO	OS Identification	General	1		
INFO	OS Security Pat...	Settings	1		
INFO	Service Detection	Service detection	1		

INFO	OS Identification	General	1		
INFO	OS Security Pat...	Settings	1		
INFO	Service Detection	Service detection	1		
INFO	Target Credenti...	Settings	1		
INFO	TCP/IP Timesta...	General	1		
INFO	Traceroute Info...	General	1		
INFO	WMI Not Availa...	Windows	1		
INFO	WS-Manageme...	Web Servers	1